Przykład

Wyznaczyć najmniejszą liczbę naturalną spełniającą układ kongruencji
$\begin{cases} x \equiv_6 1 \\ x \equiv_{11} 6 \end{cases}.$
Zauważmy, że mamy $m_1 = 6$, $m_2 = 11$, $r_1 = 1$ i $r_2 = 6$.
Chińskie twierdzenie o resztach orzeka, że najmniejsze naturalne rozwiązanie układu jest liczbą mniejszą od 66.
$M_1 = 11$ i $M_2 = 6$. Otrzymujemy równania

$$11 \cdot N_1 \equiv_6 1 \text{ oraz } 6 \cdot N_2 \equiv_{11} 6.$$

Rozwiązaniami powyższych równań są $N_1 = 5$ oraz $N_2 = 1$. Zatem

$$x = 5 \cdot 11 + 1 \cdot 6 = 61.$$

Stwierdzenie

Relacja przystawania modulo m w pierścieniu liczb całkowitych jest **kongruencją**, to znaczy jest relacją równoważności (zwrotna, symetryczna, przechodnia) oraz dla dowolnych liczb całkowitych a, b, c, d takich, że $a \equiv_m b$ i $c \equiv_m d$ zachodzi

- $(a + c) \equiv_m (b + d)$
- $ac \equiv_m bd$

Z definicji przystawania modulo m oraz z twierdzenia o dzieleniu z resztą wynika, że każda liczba całkowita przystaje modulo m dokładnie do jednej liczby ze zbioru reszt z dzielenia przez m, czyli zbioru $\{0, 1, \ldots, m-1\}$. Każda z tych reszt określa klasę abstrakcji relacji przystawania.

Przykład

Klasy abstrakcji przystawania modulo 3:

$$[0]_3 = \{\ldots,\ -9,\ -6,\ -3,\ 0,\ 3,\ 6,\ 9,\ \ldots\}$$
$$[1]_3 = \{\ldots,\ -8,\ -5,\ -2,\ 1,\ 4,\ 7,\ 10,\ \ldots\}$$
$$[2]_3 = \{\ldots,\ -7,\ -4,\ -1,\ 2,\ 5,\ 8,\ 11,\ \ldots\}$$

Przykład

Wyznaczyć najmniejszą liczbę naturalną spełniającą układ kongruencji

$$\begin{cases} x \equiv_2 1 \\ x \equiv_3 1 \\ x \equiv_5 3 \end{cases}.$$

Z danych zadania otrzymujemy $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $r_1 = r_2 = 1$ oraz $r_3 = 3$.

Mamy $M_1 = 3 \cdot 5 = 15$, $M_2 = 2 \cdot 5 = 10$ oraz $M_3 = 2 \cdot 3 = 6$. Otrzymujemy równania

$$15 \cdot N_1 \equiv_2 1, \quad 10 \cdot N_2 \equiv_3 1, \quad 6 \cdot N_3 \equiv_5 3.$$

Rozwiązaniami powyższych równań są $N_1 = 1$, $N_2 = 1$ oraz $N_3 = 3$. Zatem

$$x = 1 \cdot 15 + 1 \cdot 10 + 3 \cdot 6 = 43 \equiv_{30} 13.$$

Ostatecznie najmniejszą liczbą naturalną spełniającą dany układ kongruencji jest 13.

Liniowe równania diofantyczne

Definicja

Równaniem diofantycznym nazywamy dowolne równanie typu

$$f(x_1, x_2, \ldots, x_n) = 0,$$

w którym szukane rozwiązanie składa się z liczb całkowitych.

Definicja

Niech $a_1, a_2, \ldots, a_n \in \mathbb{Z}/\{0\}$ i niech $b \in \mathbb{Z}$. Równanie diofantyczne postaci

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$$

o niewiadomych $x_1, x_2, \ldots, x_n$ nazywamy **liniowym równaniem diofantycznym**, a liczby $a_1, a_2, \ldots, a_n$ nazywamy współczynnikami.

Przykład

Obliczyć 7^{-1} w $\mathbb{Z}_{15}$.
Szukamy rozwiązania równania $7x = 1$ w $\mathbb{Z}_{15}$. Zauważmy, że rozwiązanie istnieje, ponieważ $7 \perp 15$.
Mnożąc obustronnie równanie $7x \equiv_{15} 1$ przez 2 otrzymujemy

$$14x \equiv_{15} 2,$$

a z faktu $14 \equiv_{15} -1$ otrzymujemy

$$-1 \cdot x \equiv_{15} 2,$$

więc

$$x \equiv_{15} -2 \equiv_{15} 13.$$

Ostatecznie $7^{-1} = 13$ w $\mathbb{Z}_{15}$.
Sprawdzenie wyniku: $7 \cdot 13 = 91 = 6 \cdot 15 + 1$.

Chińskie twierdzenie o resztach

Niech $m_1, m_2, \ldots, m_n \in \mathbb{N}/\{1\}$ będą parami względnie pierwsze oraz niech $r_1, r_2, \ldots, r_n \in \mathbb{Z}$. Wtedy układ równań

$$\begin{cases} x \equiv_{m_1} r_1 \\ x \equiv_{m_2} r_2 \\ \vdots \\ x \equiv_{m_n} r_n \end{cases}$$

ma dokładnie jedno rozwiązanie modulo $M = m_1 \cdot m_2 \cdot \ldots \cdot m_n$ postaci

$$x = N_1 M_1 + N_2 M_2 + \ldots + N_n M_n,$$

gdzie $M_i = \dfrac{M}{m_i}$ oraz N_i jest rozwiązaniem równania $M_i N_i \equiv_{m_i} r_i$ dla $i = 1, 2, \ldots, n$.

Oczywiście rozwiązania rozpatrywanego układu równań w zbiorze liczb całkowitych mają postać $x = N_1 M_1 + N_2 M_2 + \ldots + N_n M_n + Mt$, gdzie t jest dowolną liczbą całkowitą.

Twierdzenie

Niech $a, b, c, d \in \mathbb{Z}$ i $m, k \in \mathbb{N}/\{1\}$.

- $a \equiv_m b$ wtedy i tylko wtedy, gdy $ak \equiv_{mk} bk$.
- Jeżeli $a \equiv_m b$, to $ac \equiv_m bc$.
- Jeżeli $ac \equiv_m bc$ oraz $c \perp m$, to $a \equiv_m b$.
- Jeżeli $a \equiv_{mk} b$, to $a \equiv_m b$ oraz $a \equiv_k b$.
- Jeżeli $a \equiv_m b$ oraz $a \equiv_k b$ oraz $m \perp k$, to $a \equiv_{mk} b$.

Definicja

Równanie w pierścieniu reszt modulo m nazywamy **równaniem modularnym**.

Zauważmy, że <u>każde</u> równanie modularne można traktować jako równanie diofantyczne. Wynika to z faktu, że $a \equiv_m b$ wtedy i tylko wtedy, gdy istnieje liczba całkowita k taka, że $a + mk = b$.

Twierdzenie

- Równanie $ax = b$ ma rozwiązanie w $\mathbb{Z}_m$ wtedy i tylko wtedy, gdy $\mathrm{NWD}(a, m) | b$.
- Jeżeli x_0 jest rozwiązaniem równania $ax = b$ w $\mathbb{Z}_m$, to liczba różnych rozwiązań tego równania w $\mathbb{Z}_m$ wynosi $\mathrm{NWD}(a, m)$ oraz każde rozwiązanie ma postać
$$x_t = x_0 +_m t \cdot \frac{m}{\mathrm{NWD}(a, m)}$$
dla $t \in \{0, 1, \ldots, \mathrm{NWD}(a, m) - 1\}$.

Twierdzenie Eulera

Dla $a \in \mathbb{Z}$ i $m \in \mathbb{N}/\{1\}$ takich, że $a \perp m$ zachodzi

$$a^{\varphi(m)} \equiv_m 1.$$

Małe twierdzenie Fermata

Dla $a \in \mathbb{Z}$ i $p \in \mathbb{P}$ takich, że $a \perp p$ zachodzi

$$a^{p-1} \equiv_p 1.$$

Przykład

Wyznaczyć ostatnią cyfrę liczby 7^{2022}.
Zadanie jest równoważne z określeniem wartości liczby 7^{2022} modulo 10.
Zauważmy, że

$$7^2 = 49 \equiv_{10} 9 \equiv_{10} (-1).$$

Zatem

$$7^{2022} \equiv_{10} (7^2)^{1011} \equiv_{10} (-1)^{1011} = -1 \equiv_{10} 9.$$

Ostatnią cyfrą liczby 7^{2022} jest 9.

Na zbiorze $\mathbb{Z}_m$ klas abstrakcji relacji przystawania modulo m definiujemy działania

- dodawanie modulo m:
$$[a]_m +_m [b]_m = [a+b]_m$$
- mnożenie modulo m:
$$[a]_m \cdot_m [b]_m = [a \cdot b]_m$$

Przykład

$5 +_6 2 = 1$, $4 \cdot_8 6 = 0$.

Twierdzenie

Zbiór $\mathbb{Z}_m$ klas abstrakcji relacji przystawania modulo m z działaniami dodawania modulo m i mnożenia modulo m jest pierścieniem przemiennym z jedynką, który nazywamy **pierścieniem reszt modulo** m.

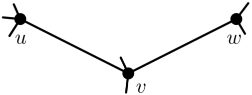
Oznaczenie

Rząd grafu oznaczamy przez n, a jego rozmiar przez m. Krawędź $\{u, v\}$ będziemy często zapisywać w postaci uv.

Definicja

Dany jest graf G i wierzchołki $u, v, w \in V(G)$.

- Jeżeli $uv \in E(G)$, to u nazywamy **wierzchołkiem sąsiednim** do v i do krawędzi uv. Krawędź uv nazywamy **krawędzią sąsiednią** do wierzchołka u i do wierzchołka v.
- Jeżeli $uv, vw \in E(G)$, to uv jest **krawędzią sąsiednią** do krawędzi vw.



Na powyższym rysunku przedstawiono fragment grafu, w którym

- wierzchołki u i v są sąsiednie, bo istnieje krawędź uv,
- wierzchołki v i w są sąsiednie, bo istnieje krawędź vw,
- wierzchołki u i w nie są sąsiednie, bo nie istnieje krawędź uw,
- krawędzie uv i vw są sąsiednie, bo mają wspólny wierzchołek v.

Definicja

Multigrafem (**grafem z krawędziami wielokrotnymi**) nazywamy graf, w którym krawędzie mogą się powtarzać ($E(G)$ jest multizbiorem).

Definicja

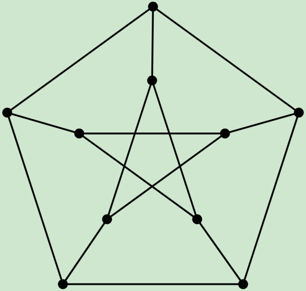
Niech $G = \big(V(G), E(G)\big)$ będzie grafem.

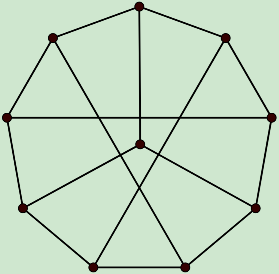
- **Drogą** nazywamy ciąg wierzchołków $(v_1, v_2, \dots, v_n)$ w grafie G taki, że $v_i v_{i+1} \in E(G)$ dla każdego $1 \leqslant i \leqslant n-1$.
- **Ścieżką** nazywamy drogę w której każdy wierzchołek występuje co najwyżej jeden raz.
- **Cyklem** nazywamy drogę w której $v_1 = v_n$ oraz wszystkie pozostałe wierzchołki występują co najwyżej jeden raz.
- **Cyklem niewłaściwym** nazywamy drogę w której $v_1 = v_n$.
- Graf G jest **spójny**, gdy dla każdej pary jego wierzchołków istnieje ścieżka zawierająca te wierzchołki.
- Maksymalny (w sensie zawierania) podgraf spójny danego grafu nazywamy **składową spójności**.

Izomorfizm grafów

Przykład

Czy można uznać poniższe rysunki za dwie różne reprezentacje graficzne tego samego grafu?





Tak!

Graf w powyższym przykładzie to tzw. *graf Petersena*.

Definicja

Grafem nazywamy parę zbiorów $G = \big(V(G), E(G)\big)$, gdzie $V(G)$ to **zbiór wierzchołków**, a $E(G)$ (**zbiór krawędzi**) to zbiór nieuporządkowanych par elementów zbioru $V(G)$.

Parę zbiorów spełniającą powyższą definicję nazywa się niekiedy **grafem nieskierowanym**.

Definicja

- **Rzędem grafu** G nazywamy liczbę jego wierzchołków $|V(G)|$.
- **Rozmiarem grafu** G nazywamy liczbę jego krawędzi $|E(G)|$.
- Wierzchołki x i y nazywamy **końcami krawędzi** $\{x, y\}$.
- Krawędź $\{x, x\}$ nazywamy **pętlą**.

Przykład

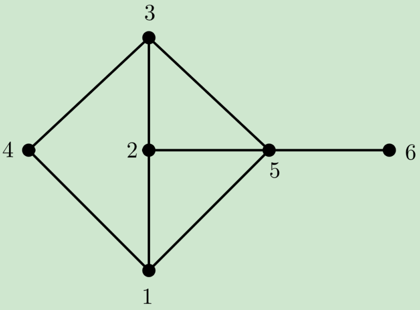
Rząd grafu G z przykładu 1 wynosi 6, a jego rozmiar to 8.

Przykład 1

Rozpatrzmy parę zbiorów:

$$V(G) = \{1,2,3,4,5,6\},$$
$$E(G) = \Big\{\{1,2\},\ \{1,4\},\ \{1,5\},\{2,3\},\ \{2,5\},\ \{3,4\},\ \{3,5\},\ \{5,6\}\Big\}.$$

Jak można przedstawić graficznie te zbiory? Przykładowa reprezentacja to:

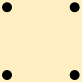


Podstawowe grafy proste

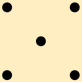
Graf pusty E_n

$V(E_n) = \{1, 2, \ldots, n\}$,
$E(E_n) = \emptyset$.

E_1



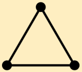
E_4



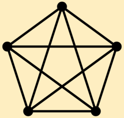
E_5

Graf pełny (klika) K_n

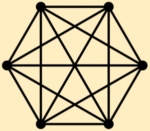
$V(K_n) = \{1, 2, \ldots, n\}$,
$E(K_n) = \{\{i, j\} : i, j \in V(K_n),\ i \neq j\}$.



K_3



K_5



K_6

Inne

- **Graf dwudzielny** - graf w którym zbiór wierzchołków można podzielić na dwa rozłączne podzbiory V_1, V_2 takie, że

$$E(G) \subset \big\{\{i,j\} : \ i \in V_1, \ j \in V_2\big\}.$$

- **Drzewo** - graf spójny nie zawierający cykli.
- **Las** - graf nie zawierający cykli.
- **Graf r-regularny** - graf w którym stopień każdego wierzchołka wynosi r.

Definicja

Jeżeli $\deg v = 1$ dla pewnego wierzchoła $v \in V(G)$, to v nazywamy **liściem**.

Teoria grafów — podstawy

dr inż. Bartłomiej Pawlik

9 września 2024

Dowód. *(2/2)*

($\Leftarrow$)
Zakładamy, że G nie zawiera cyklu nieparzystej długości.

Graf G jest dwudzielny wtedy i tylko wtedy, gdy każda jego składowa jest grafem dwudzielnym, więc możemy założyć, że G jest spójny.

Niech $x \in V(G)$ i niech V_1 będzie zbiorem wierzchołków, których odległość od x jest nieparzysta i niech $V_2 = V \backslash V_1$. Nie ma krawędzi łączących dwa wierzchołki ze zbioru V_i, bo gdyby taka krawędź istniała, to G zawierałby cykl nieparzystej długości. Zatem G jest dwudzielny.

$\square$